

# NILPOTENT AND ABELIAN HOPF-GALOIS STRUCTURES ON FIELD EXTENSIONS

NIGEL P. BYOTT

**ABSTRACT.** Let  $L/K$  be a finite Galois extension of fields with group  $\Gamma$ . When  $\Gamma$  is nilpotent, we show that the problem of enumerating all nilpotent Hopf-Galois structures on  $L/K$  can be reduced to the corresponding problem for the Sylow subgroups of  $\Gamma$ . We use this to enumerate all nilpotent (resp. abelian) Hopf-Galois structures on a cyclic extension of arbitrary finite degree. When  $\Gamma$  is abelian, we give conditions under which every abelian Hopf-Galois structure on  $L/K$  has type  $\Gamma$ . We also give a criterion on  $n$  such that *every* Hopf-Galois structure on a cyclic extension of degree  $n$  has cyclic type.

## 1. INTRODUCTION AND STATEMENT OF RESULTS

Let  $\Gamma$  be a finite group and let  $L/K$  be a finite extension of fields with  $\text{Gal}(L/K) \cong \Gamma$  (for brevity, we say:  $L$  is a  $\Gamma$ -extension of  $K$ ). Then  $L$  is a module over the group algebra  $K[\Gamma]$ , and  $K[\Gamma]$  carries the structure of a  $K$ -Hopf algebra. This makes  $L$  into a  $K[\Gamma]$ -Hopf-Galois extension of  $K$ . There may be other  $K$ -Hopf algebras  $H$  which act on  $L$  so that  $L$  is an  $H$ -Hopf-Galois extension. Such Hopf-Galois structures were investigated by Greither and Pareigis [GP], who showed how the determination of all Hopf-Galois structures on a given separable field extension  $L/K$  could be reduced to a question in group theory. In particular, any Hopf algebra  $H$  which gives a Hopf-Galois structure on  $L$  has the property that  $L \otimes_K H = L[G]$  as  $L$ -Hopf algebras, where  $G$  is some regular group of permutations of  $\Gamma$ . Thus  $G$  and  $\Gamma$  have the same order, but in general they need not be isomorphic. We will refer to the isomorphism class of  $G$  as the *type* of the Hopf-Galois structure, and will say that the Hopf-Galois structure is *abelian* (resp. *nilpotent*) if  $G$  is abelian (resp. nilpotent).

For some groups  $\Gamma$  it is known that every Hopf-Galois structure on a  $\Gamma$ -extension must have type  $\Gamma$ . This holds for cyclic groups of order  $p^n$  with  $p > 2$  prime and  $n \geq 1$  [K], for elementary abelian groups of order  $p^2$  with  $p > 2$  [B1], for cyclic groups of order  $n$  with  $(n, \varphi(n)) = 1$  (where  $\varphi$  is Euler's totient function) [B1], and for non-abelian simple

---

*Date:* October 8, 2012.

*1991 Mathematics Subject Classification.* 12F10, 16T05.

*Key words and phrases.* Hopf-Galois structure, field extension, abelian group, nilpotent group.

groups [B3]. On the other hand, there are many groups  $\Gamma$  for which there are Hopf-Galois structures whose type is different from  $\Gamma$ , the smallest cases being the two groups of order 4 [B1]. Indeed, if  $\Gamma$  is abelian then there may be Hopf-Galois structures which are not abelian, or even nilpotent. For example, if  $\Gamma$  is cyclic of order  $pq$ , where  $p, q$  are primes such that  $q \nmid (p-1)$ , then  $L/K$  admits  $2(q-1)$  Hopf-Galois structures which are not nilpotent, in addition to the unique (classical) one of type  $\Gamma$  [B2]. This phenomenon was investigated in some detail in [BC], where it was shown that any abelian extension  $L/K$  of even degree  $n > 4$  admits a non-abelian Hopf-Galois structure, and that the same holds for many abelian groups of odd order. On the other hand, some new groups  $\Gamma$  were given in [BC] for which all Hopf-Galois structures are of type  $\Gamma$  (cf. Remark 4.3 below).

In this paper, we supplement the results of [BC] by considering the situation where  $\Gamma$  and  $G$  are both abelian or, more generally, both nilpotent. We will show that the enumeration of such Hopf-Galois structures can be reduced to the case of groups of prime power order.

Let  $e(\Gamma, G)$  denote the number of Hopf-Galois structures of type  $G$  on a  $\Gamma$ -extension  $L/K$ . Thus the total number of Hopf-Galois structures on  $L/K$  is given by

$$e(\Gamma) = \sum_G e(\Gamma, G),$$

where the sum is over all isomorphism classes of groups  $G$  of order  $|\Gamma|$ . We also write

$$e_{\text{ab}}(\Gamma) = \sum_{G \text{ abelian}} e(\Gamma, G), \quad e_{\text{nil}}(\Gamma) = \sum_{G \text{ nilpotent}} e(\Gamma, G),$$

where the sum is over all isomorphism types of abelian (resp. nilpotent) groups  $G$  of order  $|\Gamma|$ . Thus  $e_{\text{ab}}(\Gamma)$  (resp.  $e_{\text{nil}}(\Gamma)$ ) is the number of abelian (resp. nilpotent) Hopf-Galois structures on  $L/K$ . Recall that a finite group  $\Delta$  is nilpotent if it is the direct product of its Sylow subgroups [R, (5.2.4)]. In particular, if  $\Delta$  is abelian, or if  $\Delta$  is a  $p$ -group for some prime number  $p$ , then  $\Delta$  is nilpotent.

Let  $n$  be the degree of the extension  $L/K$ . We write the prime factorisation of  $n$  as

$$n = \prod_{p|n} p^{v_p},$$

where the product is over the distinct prime factors  $p$  of  $n$ . If  $\Gamma$  is nilpotent, we can correspondingly write  $\Gamma$  as a direct product of groups

$$(1) \quad \Gamma = \prod_{p|n} \Gamma_p,$$

where  $\Gamma_p$  is the (unique) Sylow  $p$ -subgroup of  $\Gamma$  and has order  $p^{v_p}$ . By Galois theory, we can then decompose  $L$  as

$$L = \bigotimes_{p|n} L_p,$$

(tensor product over  $K$ ) where  $L_p$  is a  $\Gamma_p$ -extension of  $K$ . If, for each  $p$ , we take a Hopf-Galois structure on  $L_p/K$ , say of type  $G_p$  and with corresponding  $K$ -Hopf algebra  $H_p$ , then the Hopf algebra  $H = \bigotimes_{p|n} H_p$  acts in the obvious way on  $L$ , giving  $L/K$  a Hopf-Galois structure of type  $G = \prod_{p|n} G_p$ . This Hopf-Galois structure is necessarily nilpotent, and is abelian if and only if each  $G_p$  is abelian.

We will see that if  $\Gamma$  is nilpotent then *every* nilpotent Hopf-Galois structure on  $L/K$  arises in this way. This is the key observation in the proof of our first main result:

**THEOREM 1.** *Let  $\Gamma$  be a nilpotent group of order  $n$ . Then for each nilpotent group  $G$  of order  $n$  we have  $e(\Gamma, G) = \prod_{p|n} e(\Gamma_p, G_p)$ .*

Taking the sum over all isomorphism types of nilpotent (resp. abelian) groups  $G$  of order  $n$ , we immediately obtain:

**COROLLARY 1.1.** *For a finite nilpotent group  $\Gamma$ , we have*

$$e_{\text{nil}}(\Gamma) = \prod_{p|n} e(\Gamma_p) \text{ and } e_{\text{ab}}(\Gamma) = \prod_{p|n} e_{\text{ab}}(\Gamma_p).$$

As an application of Theorem 1, we will determine the number of nilpotent (resp. abelian) Hopf-Galois structures on a cyclic extension of arbitrary finite degree. Before stating the result, we fix some notation. For  $m \geq 1$ , let  $C_m$  denote the cyclic group of order  $m$ , and, for  $v \geq 3$ , let  $D_{2^v}$  (resp.  $Q_{2^v}$ ) denote the dihedral (resp. generalized quaternion) group of order  $2^v$ . Also, for  $n \geq 1$ , let  $r(n)$  be the radical of  $n$ :

$$r(n) = \prod_{p|n} p.$$

**THEOREM 2.** *Let  $\Gamma$  be a cyclic group of order  $n$ .*

(i) *If  $n$  is not divisible by 4, then*

$$e_{\text{nil}}(\Gamma) = e_{\text{ab}}(\Gamma) = e(\Gamma, \Gamma) = \frac{n}{r(n)}.$$

*Thus every nilpotent Hopf-Galois structure on a cyclic extension of degree  $n$  is cyclic, and hence abelian.*

(ii) *If  $n \equiv 4 \pmod{8}$ , then again*

$$e_{\text{nil}}(\Gamma) = e_{\text{ab}}(\Gamma) = \frac{n}{r(n)},$$

*but*

$$e(\Gamma, \Gamma) = e(\Gamma, C_2 \times C_{n/2}) = \frac{n}{2r(n)}.$$

*Thus every nilpotent Hopf-Galois structure on a cyclic extension of degree  $n$  is abelian, but only half of them are cyclic.*

(iii) *If  $n$  is divisible by 8, so  $n = 2^v n'$  with  $v \geq 3$  and  $n'$  odd, then*

$$e_{\text{nil}}(\Gamma) = \frac{3n}{2r(n)} \text{ and } e_{\text{ab}}(\Gamma) = e(\Gamma, \Gamma) = \frac{n}{2r(n)},$$

*with*

$$e(\Gamma, D_{2^v} \times C_{n'}) = e(\Gamma, Q_{2^v} \times C_{n'}) = \frac{n}{2r(n)},$$

*Thus every abelian Hopf-Galois structure on a cyclic extension of degree  $n$  is cyclic, although there are also Hopf-Galois structures which are nilpotent but not abelian.*

For a finite abelian  $p$ -group  $\Gamma$ , Featherstonhaugh, Caranti and Childs [FCC] have given conditions under which every abelian Hopf-Galois structure on a  $\Gamma$ -extension must have type  $\Gamma$ . Combining this with Theorem 1, we will obtain the following result in the abelian case.

**THEOREM 3.** *Let  $\Gamma$  be a finite group of order  $n = \prod_p p^{v_p}$ , and suppose that, for each prime factor  $p$  of  $n$ , either  $v_p < p - 1$  or  $p \leq 3$ ,  $v_p < p$ . Then every abelian Hopf-Galois structure on a  $\Gamma$ -extension has type  $\Gamma = \text{Gal}(L/K)$ . Equivalently,  $e_{\text{ab}}(\Gamma) = e(\Gamma, \Gamma)$ .*

Combining Theorems 2 and 3 with a result of L. E. Dickson [D] dating from 1905, we obtain some new cyclic groups  $\Gamma$  for which every Hopf-Galois structure has type  $\Gamma$ :

**THEOREM 4.** *Suppose that  $n = \prod_p p^{v_p}$  satisfies the following conditions:*

- (i)  $v_p \leq 2$  for all primes  $p$  dividing  $n$ ;
- (ii)  $p \nmid (q^{v_q} - 1)$  for all primes  $p, q$  dividing  $n$ ;
- (iii)  $4 \nmid n$ .

*Then a cyclic extension of degree  $n$  admits precisely  $n/r(n)$  Hopf-Galois structures, all of which are of cyclic type.*

**ACKNOWLEDGMENT:** The author thanks Lindsay Childs and Tim Kohl for email correspondence about this work, which led to a simplification of some of the arguments.

## 2. NILPOTENT HOPF-GALOIS STRUCTURES

In this section we prove Theorem 1.

We first recall the method of counting Hopf-Galois structures on a  $\Gamma$ -extension for an arbitrary finite group  $\Gamma$ . It was shown in [GP] that these Hopf-Galois structures correspond to regular permutation groups on  $\Gamma$  which are normalized by the group  $\lambda(\Gamma)$  of left multiplications by elements of  $\Gamma$ . (Recall that a permutation group  $H$  on a set  $X$  is regular if, given  $x, y \in X$ , there is a unique  $h \in H$  with  $hx = y$ .) Thus finding

all Hopf-Galois structures with a given type  $G$  amounts to finding all regular subgroups in the group  $\text{Perm}(\Gamma)$  of permutations of  $\Gamma$  which are isomorphic to  $G$  and are normalized by  $\lambda(\Gamma)$ . It was shown in [B1] that this problem can be reframed as a calculation inside  $\text{Hol}(G) = \rho(G) \cdot \text{Aut}(G)$ , the holomorph of  $G$ , which is usually a much smaller group than  $\text{Perm}(\Gamma)$ . Here  $\rho : G \rightarrow \text{Perm}(G)$  is the right regular representation  $\rho(g)(x) = xg^{-1}$  for  $g, x \in G$ . As further reformulated by Childs (see e.g. [C, §7]), this gives the following method of counting Hopf-Galois structures. A homomorphism  $\beta : \Gamma \rightarrow \text{Hol}(G)$  will be called a regular embedding if it is injective and its image is a regular group of permutations on  $G$ . Two such embeddings will be called equivalent if they are conjugate by an element of  $\text{Aut}(G)$ . Then the number  $e(\Gamma, G)$  of Hopf-Galois structures of type  $G$  on a  $\Gamma$ -extension is the number of equivalence classes of regular embeddings of  $\Gamma$  into  $\text{Hol}(G)$ .

We will need the following general result.

**PROPOSITION 2.1.** *Let  $N$  be a regular subgroup of  $\text{Hol}(G)$ . Then the centralizer of  $N$  in  $\text{Hol}(G)$  has order dividing  $|G|$ .*

*Proof.* We can regard  $\text{Hol}(G)$  as a subgroup of the group  $B = \text{Perm}(G)$  of all permutations of  $G$ . By [GP, Lemma 2.4.2], the centralizer of  $N$  in  $B$  is canonically identified with the opposite group of  $N$ , so in particular has order  $|N| = |G|$ . The centralizer of  $N$  in  $\text{Hol}(G)$  is a subgroup of this, so has order dividing  $|G|$ .  $\square$

If  $G$  is a nilpotent group, its Sylow subgroups  $G_p$  are characteristic subgroups. We therefore have direct product decompositions

$$(2) \quad \text{Aut}(G) = \prod_{p|n} \text{Aut}(G_p),$$

and hence

$$(3) \quad \text{Hol}(G) = \prod_{p|n} \text{Hol}(G_p).$$

Now suppose that  $\Gamma$  and  $G$  are nilpotent groups of order  $n$ , and that we are given a homomorphism  $\beta_p : \Gamma_p \rightarrow \text{Hol}(G_p)$  for each  $p|n$ . Using (1) and (3), we can define a homomorphism

$$(4) \quad \beta = \left( \prod_{p|n} \beta_p \right) : \Gamma \rightarrow \text{Hol}(G).$$

It is clear that if each  $\beta_p$  is a regular embedding then so is  $\beta$ . This construction corresponds to taking tensor products of Hopf-Galois structures on field extensions of prime-power degrees, as described in §1.

Not every homomorphism  $\beta : \Gamma \rightarrow \text{Hol}(G)$  arises as such a product. For any primes  $p, q$  dividing  $n$ , let  $\iota_p : \Gamma_p \rightarrow \Gamma$  be the inclusion induced

by the direct product decomposition (1) of  $\Gamma$ , and let  $\pi_q: \text{Hol}(G) \rightarrow \text{Hol}(G_q)$  be the projection induced by (3). Given a homomorphism  $\beta: \Gamma \rightarrow \text{Hol}(G)$ , let  $\beta_{pq}$  be the composite homomorphism  $\beta_{pq} = \pi_q \circ \beta \circ \iota_p: \Gamma_p \rightarrow \text{Hol}(G_q)$ . Then  $\beta$  is determined by its matrix of components  $(\beta_{pq})$ . For each  $q$ , the images of the  $\beta_{pq}$  must centralize each other in  $\text{Hol}(G_q)$ , since the  $\Gamma_p$  centralize each other in  $\Gamma$ . Conversely, a matrix of homomorphisms  $(\beta_{pq})$ ,  $\beta_{pq}: \Gamma_p \rightarrow \text{Hol}(G_q)$ , determines a homomorphism  $\beta: \Gamma \rightarrow \text{Hol}(G)$ , provided only that, for each  $q$ , the images of the  $\beta_{pq}$  centralize each other in  $\text{Hol}(G_q)$ .

We can determine from the matrix  $(\beta_{pq})$  whether  $\beta$  is a regular embedding:

**LEMMA 2.2.** *Let  $\Gamma$  and  $G$  be nilpotent, and let  $\beta: \Gamma \rightarrow G$  correspond to the matrix of homomorphisms  $(\beta_{pq})$  as above. Then  $\beta$  is a regular embedding if and only if  $\beta_{pp}: \Gamma_p \rightarrow \text{Hol}(G_p)$  is a regular embedding for each  $p$ .*

*Proof.* First observe that  $\beta_{pp}(\Gamma_p)$  is the unique Sylow  $p$ -subgroup in the subgroup  $\pi_p \circ \beta(\Gamma)$  of  $\text{Hol}(G_p)$ , and hence is normal in  $\pi_p \circ \beta(\Gamma)$ .

If  $\beta$  is regular then  $\pi_p \circ \beta(\Gamma)$  is transitive on  $G_p$ . Then, by Proposition 2.3 below, the number of orbits of  $\beta_{pp}(\Gamma_p)$  on  $G_p$  divides both  $|G_p| = p^{v_p}$  and  $|\pi_p \circ \beta(\Gamma)/\beta_{pp}(\Gamma)|$  (which is coprime to  $p$ ). Thus  $\beta_{pp}$  is transitive, and hence regular, on  $G_p$ .

Conversely, suppose that each  $\beta_{pp}$  is a regular embedding. We write  $e_G$  for the identity element of  $G$ . Consider the subsets  $X = \beta(\Gamma)e_G$  and  $Y = \beta(\Gamma_p)e_G$  of  $G$ . Clearly  $|Y| \leq |\Gamma_p|$ , and the regularity of  $\beta_{pp}$  ensures that  $|Y| \geq |G_p| = |\Gamma_p|$ . Hence  $|Y| = |\Gamma_p|$ . As  $\beta(\Gamma_p)$  is normal in  $\beta(\Gamma)$ , Proposition 2.3 shows that all orbits of  $\beta(\Gamma_p)$  on  $X$  have the same size. One such orbit is  $Y$ , so  $|X|$  is divisible by  $|\Gamma_p|$ . This holds for all  $p$ , so  $X = G$  and  $\beta$  is a regular embedding.  $\square$

In the above proof, we used the following simple fact about permutation groups:

**PROPOSITION 2.3.** *Let  $H$  be a finite group acting transitively on a set  $X$ , and let  $N$  be a normal subgroup of  $H$ . Then the orbits of  $N$  on  $X$  all have the same size, and the number of these orbits divides both  $|X|$  and  $|H/N|$ .*

*Proof.* Let  $N$  have  $m$  orbits on  $X$ , and let  $Nx$  and  $Ny$  be two such orbits. Then  $y = hx$  for some  $h \in H$ , and  $Ny = Nhx = hNx$ . This shows that the quotient group  $H/N$  acts on the set  $\{Nx\}$  of orbits of  $N$ , and that this action is transitive. It follows firstly that these orbits have the same size, so that  $m$  divides  $|X|$ , and secondly that  $m$  divides  $|H/N|$ .  $\square$

*Proof of Theorem 1.* Let  $\beta: \Gamma \rightarrow \text{Hol}(G)$  be a regular embedding, and let  $(\beta_{pq})$  be the corresponding matrix of homomorphisms.

By Lemma 2.2, each  $\beta_{pp}$  is a regular embedding of  $\Gamma_p$  into  $\text{Hol}(G_p)$ . For  $p \neq q$ , the image of the homomorphism  $\beta_{pq}: \Gamma_p \rightarrow \text{Hol}(G_q)$  must centralize the regular subgroup  $\beta_{qq}(\Gamma_q)$  of  $\text{Hol}(G_q)$ , and so must be a  $q$ -group by Proposition 2.1. But  $\beta_{pq}(\Gamma_p)$  is a  $p$ -group since  $\Gamma_p$  is. Thus  $\beta_{pq}$  is the trivial homomorphism whenever  $p \neq q$ . This means that the matrix  $(\beta_{pq})$  is “diagonal” and  $\beta$  is just the product  $\beta = (\prod_p \beta_{pp})$  as in (4). Conversely, given a regular embedding  $\beta_p: \Gamma_p \rightarrow \text{Hol}(G_p)$  for each  $p$ , the homomorphism  $(\prod_p \beta_p): \Gamma \rightarrow G$  is a regular embedding. It is immediate that these two constructions are mutually inverse.

We have just established a bijection between regular embeddings  $\beta: \Gamma \rightarrow \text{Hol}(G)$  and families of regular embeddings  $\beta_p: \Gamma_p \rightarrow \text{Hol}(G_p)$  for each  $p|n$ . It follows from (2) that two regular embeddings  $\beta, \beta'$  are conjugate by an element of  $\text{Aut}(G)$  if and only if, for each  $p$ , their components  $\beta_p, \beta'_p$  are conjugate by an element of  $\text{Aut}(G_p)$ . Hence the equivalence classes of regular embeddings  $\beta: \Gamma \rightarrow \text{Hol}(G)$  correspond bijectively to families of equivalence classes of regular embeddings  $\beta_p: \Gamma_p \rightarrow \text{Hol}(G_p)$ . This shows that  $e(\Gamma, G) = \prod_p e(\Gamma_p, G_p)$ .  $\square$

### 3. HOPF-GALOIS STRUCTURES ON CYCLIC EXTENSIONS

For cyclic extensions whose degree is a power of a prime  $p$ , all the Hopf-Galois structures are already known. We recall the results.

- LEMMA 3.1. (i) For  $n = p^v$  with  $p > 2$  and  $v \geq 1$ , we have  $e(C_n) = e(C_n, C_n) = p^{v-1}$ .  
(ii) For  $n = 2$ , we have  $e(C_2) = e(C_2, C_2) = 1$ ; for  $n = 4$ , we have  $e(C_4) = 2$  with  $e(C_4, C_4) = e(C_4, C_2 \times C_2) = 1$ .  
(iii) For  $n = 2^v$  with  $v \geq 3$ , we have  $e(C_n) = 3 \cdot 2^{v-2}$  with  $e(C_n, C_n) = e(C_n, D_n) = e(C_n, Q_n) = 2^{v-2}$ .

Thus, for a prime power  $n = p^v$ , we have  $e(C_n) = n/r(n)$  except in the case  $p = 2, v \geq 3$ , when  $e(C_n) = 3n/(2r(n))$ .

*Proof.* (i) is equivalent to Kohl’s result [K] that, for an odd prime  $p$ , a cyclic Galois extension of degree  $p^r$  admits  $p^{r-1}$  Hopf-Galois structures, all of cyclic type. Similarly, (ii) follows from [B1] and (iii) from [B4].  $\square$

Theorem 2 follows directly from Lemma 3.1 and Theorem 1.

### 4. ABELIAN HOPF-GALOIS STRUCTURES

In this section, we prove Theorems 3 and 4.

From [FCC, Theorem 1] we have the following result:

- LEMMA 4.1. Let  $\Gamma$  be an abelian  $p$ -group of  $p$ -rank  $m$ , with  $p > m + 1$ . Then  $e_{\text{ab}}(\Gamma) = e(\Gamma, \Gamma)$ .

*Proof of Theorem 3.* Let  $G$  be an abelian group of order  $n$ , and let  $\Gamma_p, G_p$  be the Sylow  $p$ -subgroups of  $\Gamma, G$  as usual. If  $v_p < p - 1$  then certainly  $p > m + 1$  where  $m$  is the  $p$ -rank of  $G_p$ , so, by Lemma 4.1,  $e(\Gamma_p, G_p) = 0$  unless  $G_p = \Gamma_p$ . If  $p = 3$  and  $v_3 = 2$  then either  $\Gamma_3 = C_9$ , when by Lemma 3.1(i) we have  $e(\Gamma_3, G_3) = 0$  unless  $G_3 = \Gamma_3$ , or  $\Gamma_3 = C_3 \times C_3$ , when the same conclusion holds by [B1]. If  $p = 2$  and  $v_2 = 1$  then  $\Gamma_2 = C_2$  and  $G_2 = C_2$ . Thus the hypotheses of Theorem 3 ensure that  $e_{\text{ab}}(\Gamma_p) = e(\Gamma_p, \Gamma_p)$  for all  $p$ . By Corollary 1.1 we then have

$$e_{\text{ab}}(\Gamma) = \prod_{p|n} e(\Gamma_p, \Gamma_p) = e(\Gamma, \Gamma),$$

and every abelian Hopf-Galois structure on  $L/K$  has type  $\Gamma$ .  $\square$

To prove Theorem 4, we need the following old result of L. E. Dickson [D] (see also [DF, §5.5, Exercise 24, p. 189]):

**LEMMA 4.2.** *Let  $n$  have prime factorisation  $\prod_p p^{v_p}$ . Then every group of order  $n$  is abelian if and only if  $v_p \leq 2$  for each prime  $p$  dividing  $n$ , and  $p \nmid (q^{v_q} - 1)$  for all primes  $p, q$  dividing  $n$ .*

*Proof of Theorem 4.* Let  $\Gamma$  be a cyclic group of order  $n$ . The conditions of Theorem 4 imply those of Theorem 3, so that every abelian Hopf-Galois structure on a  $\Gamma$ -extension has cyclic type. On the other hand, the hypotheses of Lemma 4.2 are also satisfied. Thus every group of order  $n$  is abelian, and therefore every Hopf-Galois structure is abelian. It follows that all the Hopf-Galois structures are cyclic. By Theorem 2(i), the number of Hopf-Galois structures is therefore  $n/r(n)$ .  $\square$

**REMARK 4.3.** *In Theorem 4, there are no non-abelian Hopf-Galois structures for the rather trivial reason that there are no non-abelian groups of the appropriate order. This result is certainly not best possible, since if  $n = p^2 q^2$  for primes  $2 < q < p$  with  $(q, p + 1) > 1$  (e.g.  $q = 3, p = 11$ ), or if  $n = p^3 q$  for distinct primes  $p, q$  with  $(p, q - 1) = (q, p^2 - 1) = 1$  but  $(q, p^3 - 1) > 1$  (e.g.  $p = 7, q = 19$ ), then a cyclic extension of degree  $n$  admits only cyclic Hopf-Galois structures [BC, Theorems 24, 25]. In both cases, non-abelian groups of order  $n$  exist, but a partial analysis of their holomorphs shows that they cannot arise as the type of a Hopf-Galois structure on a cyclic extension.*

## 5. ABELIAN HOPF-GALOIS STRUCTURES ON ABELIAN EXTENSIONS

In this final section we describe an alternative approach to Theorem 1 in the case that  $\Gamma$  and  $G$  are both abelian (restated as Theorem 5 below). This avoids the use of Proposition 2.1, and instead is based upon a result of Caranti, Dalla Volta and Sala [CDVS] which underlies



Lemma 4.1. It therefore shows how the ideas in [FCC] extend to a finite abelian group  $\Gamma$  which is not of prime-power order.

An important ingredient in the proof of Lemma 4.1 (though not of the original weaker version in Featherstonhaugh's thesis [F]) is a correspondence between regular subgroups of  $\text{Hol}(G)$  for an abelian group  $G$  and certain multiplication operations  $\cdot$  on  $G$ . This correspondence was first observed in [CDVS, Theorem 1] for vector spaces over a field  $F$ . The case  $F = \mathbb{F}_p$  (the field of  $p$  elements) covers elementary abelian  $p$ -groups  $G$ . It was noted in [FCC] that the same argument works for any finite  $p$ -group; indeed, this is what is required to prove Lemma 4.1. It is easily verified that the argument of [CDVS] is still valid for arbitrary abelian groups. Here is the result in that setting.

LEMMA 5.1. *Let  $(G, +)$  be an abelian group with identity element 0. Then there is a one-to-one correspondence between regular abelian subgroups  $T$  of  $\text{Hol}(G)$  and binary operations  $\cdot$  on  $G$  which make  $(G, +, \cdot)$  into a commutative, associative (non-unital) ring with the property that every element of  $G$  has an inverse under the circle operation  $x \circ y = x + y + x \cdot y$  (so  $(G, \circ)$  is an abelian group, whose identity element is again 0). Under this correspondence, the subgroup  $T$  of  $\text{Hol}(G)$  corresponding to  $\cdot$  is  $\{\tau_g : g \in G\}$ , where  $\tau_g(x) = g \circ x$  for all  $x \in G$ .*

We next investigate the Sylow subgroups of (the additive group of) such a ring.

PROPOSITION 5.2. *Let  $(R, +, \cdot)$  be a finite associative non-unital ring, and for each prime  $p$  dividing its order, let  $R_p$  be the Sylow  $p$ -subgroup of  $(R, +)$ . Then  $R_p$  is an ideal (and hence a subring) of  $R$ , and  $R$  is the direct product of its subrings  $R_p$ . Moreover, every element of  $R$  has an inverse under  $\circ$  if and only if the same is true in each  $R_p$ .*

*Proof.* Let  $r \in R_p$ , and let  $s \in R$  be arbitrary. If  $p^e$  is the exponent of  $R_p$  then, by associativity,  $p^e(r \cdot s) = (p^e r) \cdot s = 0 \cdot s = 0$ , so that  $r \cdot s \in R_p$ . Similarly  $s \cdot r \in R_p$ . In particular, if  $r \in R_p$  and  $s \in R_p$  then  $r \cdot s \in R_p$ , and if  $r \in R_p$  and  $s \in R_q$  with  $p \neq q$  then  $r \cdot s \in R_p \cap R_q$  so  $r \cdot s = 0$ . Hence  $R_p$  is both an ideal and a subring of  $R$ , and  $R$  is the direct product of its subrings  $R_p$ . Suppose now that every  $r \in R$  has a  $\circ$ -inverse. If  $r \in R_p$  has  $\circ$ -inverse  $s$  in  $R$  then  $s = -r - r \cdot s \in R_p$ , so  $r$  has  $\circ$ -inverse  $s$  in  $R_p$ . Conversely, suppose that  $\circ$ -inverses exist in each  $R_p$ . Let  $r \in R$ . We can write  $r = \sum_p r_p$  with  $r_p \in R_p$  for each  $p$ . If  $s_p$  is the  $\circ$ -inverse of  $r_p$  in  $R_p$  then  $s = \sum_p s_p$  is the  $\circ$ -inverse of  $r$  in  $R$ .  $\square$

COROLLARY 5.3. *In Lemma 5.1, the Sylow  $p$ -subgroup  $T_p$  of  $T$  is  $\{\tau_g : g \in G_p\}$ .*

*Proof.* If  $g, h \in G_p$  then  $g \circ h = g + h + g \cdot h \in G_p$  by Proposition 5.2. But  $\tau_g(\tau_h(x)) = g \circ (h \circ x) = (g \circ h) \circ x = \tau_{g \circ h}(x)$ . The non-empty

subset  $\{\tau_g : g \in G_p\}$  of the finite abelian group  $T$  is therefore closed under composition, and hence is a subgroup. Since its cardinality is  $|G_p|$  and  $|G| = |T|$ , it is the Sylow  $p$ -subgroup  $T_p$ .  $\square$

**THEOREM 5.** *Let  $\Gamma$  and  $G$  be abelian groups of order  $n$ . Then*

$$e(\Gamma, G) = \prod_{p|n} e(\Gamma_p, G_p).$$

*Proof.* Let  $\beta: \Gamma \rightarrow \text{Hol}(G)$  be a regular embedding. Then  $T = \beta(\Gamma) \cong \Gamma$  is a regular subgroup of  $\text{Hol}(G)$  which by Lemma 5.1 gives a multiplication  $\cdot$  on  $G$  making  $G$  into a ring. Then  $T = \{\tau_g : g \in G\}$ , where the  $\tau_g$  are defined using the  $\circ$ -operation obtained from  $\cdot$ . By Proposition 5.2,  $G$  is the direct product of its subrings  $G_p$ . Since  $\circ$ -inverses exist in  $G$ , they exist in  $G_p$ , so that the multiplication on  $G_p$  corresponds via Lemma 5.1 to a regular subgroup  $T'_p$  of  $\text{Hol}(G_p)$ . Writing elements of  $G = \prod_p G_p$  as tuples  $g = (g_p)_p$  with  $g_p \in G_p$ , we have

$$\tau_g(x) = g + x + g \cdot x = (g_p + x_p + g_p \cdot x_p)_p$$

for any  $x = (x_p)_p \in G$ . It follows that  $T'_p$  consists of the restrictions to  $G_p$  of the  $\tau_{g_p}$  for  $g_p \in G_p$ . By Corollary 5.3, the  $\tau_{g_p}$  are precisely the elements of the Sylow  $p$ -subgroup  $T_p = \beta(\Gamma_p)$  of  $T$ . Thus  $\beta$  induces a regular embedding  $\beta_p: \Gamma_p \rightarrow \text{Hol}(G_p)$  for each  $p$ , where  $\beta_p(h)$  for  $h \in \Gamma_p$  is merely the restriction of  $\beta(h)$  to  $G_p$ . If we form the product  $\beta^* = \left(\prod_p \beta_p\right): \Gamma \rightarrow \text{Hol}(G)$  as in (4), then  $T^* = \beta^*(\Gamma)$  is a regular subgroup of  $\text{Hol}(G)$  which induces the operation  $\cdot$  on each  $G_p$ . By Lemma 5.1 and Proposition 5.2 we then have  $T^* = T$  and so  $\beta^* = \beta$ . Thus every regular embedding  $\beta$  comes from a family of regular embeddings  $\beta_p$ . As in the proof of Theorem 1, it follows that  $e(\Gamma, G) = \prod_p e(\Gamma_p, G_p)$ .  $\square$

## REFERENCES

- [B1] N.P. Byott, Uniqueness of Hopf Galois structure for separable field extensions. *Comm. Algebra* **24** (1996), 3217–28; Corrigendum, *ibid.* 3705.
- [B2] N.P. Byott, Hopf-Galois structures on Galois field extensions of degree  $pq$ . *J. Pure and Applied Algebra* **188**, (2004), 45–57.
- [B3] N.P. Byott, Hopf-Galois structures on field extensions with simple Galois groups. *Bull. London Math. Soc.* **36**, (2004), 23–29.
- [B4] N.P. Byott, Hopf-Galois structures on almost cyclic field extensions of 2-power degree. *J. Algebra* **318**, (2007), 351–371.
- [BC] N.P. Byott, L.N. Childs, Fixed-point free pairs of homomorphisms and nonabelian Hopf-Galois structures. *To appear in* New York J. Math.
- [CDVS] A. Caranti, F. Della Volta, M. Sala, Abelian regular subgroups of the affine group and radical rings. *Publ. Math. Debrecen* **69** (2006), 297–308 (available at [arXiv:math/0510166v2](https://arxiv.org/abs/math/0510166v2) [[math.GR](https://arxiv.org/abs/math/0510166v2)]).

- [C] L.N. Childs, *Taming Wild Extensions: Hopf Algebras and Local Galois Module Structure*. Mathematical Surveys and Monographs **80**, Amer. Math. Soc. (2000).
- [D] L.E. Dickson, Definitions of a group and a field by independent postulates. Trans. Amer. Math. Soc. **6** (1905), 198–204.
- [DF] D.S. Dummit, R.M. Foote, *Abstract Algebra*. (2nd edn.) Prentice Hall, (1999).
- [F] S.C. Featherstonhaugh, *Abelian Hopf Galois structures on Galois field extensions of prime power degree*. PhD thesis, SUNY at Albany, (2003).
- [FCC] S.C. Featherstonhaugh, A. Caranti, L.N. Childs, Abelian Hopf Galois structures on prime-power Galois field extensions. Trans. Amer. Math. Soc. **364**, (2012), 3675–3684.
- [GP] C. Greither, B. Pareigis, Hopf Galois theory for separable field extensions. J. Algebra **106**, (1987), 239–258.
- [K] T. Kohl, Classification of Hopf Galois structures on prime power radical extensions. J. Algebra **207**, (1998), 525–546.
- [R] D.J.S. Robinson, *A Course in the Theory of Groups*. Graduate Texts in Mathematics **80**, Springer, 1993.

COLLEGE OF ENGINEERING, MATHEMATICS AND PHYSICAL SCIENCES, UNIVERSITY OF EXETER, EXETER EX4 4QF U.K.

*E-mail address:* N.P.Byott@exeter.ac.uk